趨勢科技

Deep Discovery Analyzer 動態分析系統

採用客製化沙盒模擬分析來提升您對鎖定目標攻擊的防護能力

鎖定目標攻擊與進階威脅都是專為滲透您的 IT 基礎架構而客製化，不僅能躲過傳統的防禦，而且能持續躲藏在您的企業內竊取資料。傳統標準的資安防護通常無法偵測這類攻擊所使用的進階惡意程式與躲避技巧。唯有透過虛擬化模擬分析(也就是 Sandboxing 沙盒模擬分析) 在安全、隔離的環境當中實際執行並觀察可疑的檔案，才能準確地可靠地偵測並分析這類惡意程式。在您的標準防護產品當中加入沙盒模擬分析，可提升其防護價值並建立一 套整合的鎖定式目標攻擊防禦。

趨勢科技 deep discovery analyzer™ 是一套可擴充的沙盒模擬分析系統，提 供企業內沙盒模擬分析服務。Analyzer 可讓您定義多個客製化沙盒環境，也就是與桌面軟體組態相同的虛擬環境。能直接與趨勢科技電子郵件及網站防護產品整合同時亦支援 Deep Discovery 平台的其他產品。開放的網站服務 (Web Services) API，可讓第三方產品或經過授權的使用者上傳樣本做進一步的分析。

主要功能

可擴充的沙盒模擬分析服務 採用可擴充的解決方案，不僅能確保 效能最佳化，更能處理電子郵件、網 路、端點以及其他來源的樣本。

客製化沙盒模擬分析 採用與您桌面軟體組態一致的環境來 執行沙盒模擬與分析，確保最高的偵 測率並降低誤判率。

廣泛分析各種檔案 採用多重偵測引擎與沙盒模擬分析技 術來檢查各種 Windows 執行檔、 Microsoft Office 檔案、PDF、網站 內容以及壓縮檔案。。。等。

文件漏洞攻擊偵測 採用特殊的偵測引擎和沙盒模擬分析 來發掘利用一般常用文件漏洞的惡意 程式。

URL 分析
針對手動上傳的 URL 進行網頁掃瞄與沙盒模擬 分析。

詳細的報表 藉由集中式儀表板與報表，提供詳盡 分析結果，包括詳細的樣本活動與 C&C 通訊。

與趨勢科技產品整合 可直接與絕趨勢科技電子郵件及網站 防護產品。。等整合。

網站服務 API 與手動上傳 可允許第三方產品或經過授權的威脅 研究人員上傳樣本。

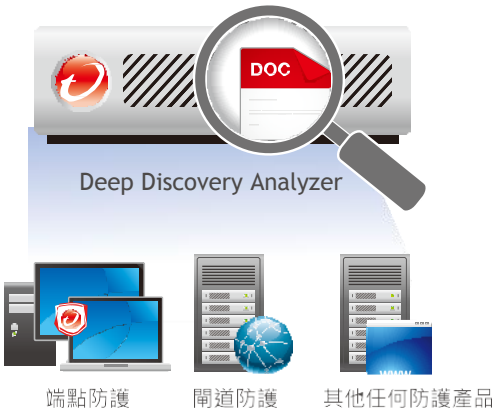
客製化防禦整合 自動與其他趨勢科技解決方案和第三 方防護產品分享最新入侵指標(IOC) 偵測情報。

主要效益

更優異的攻擊防護 讓任何防護產品擁有整合式惡意 程式沙盒模擬分析，提升防護價 值。

開放、可擴充的平台 在企業內提供高效能的進階惡意 程式偵測及分析資源。

深入的惡意程式分析 可深入調查惡意程式並彙整惡意 程式偵測報表。



為何客製化沙盒模擬分析有其必要

網路犯罪集團會針對您的特殊環境，包括您的桌上型和筆記型電腦作業系統、應用程式以及瀏覽器等等來開 發出客製化的惡意程式。既然惡意程式是針對您的系統組態而開發，因此不太可能會在通用的沙盒環境當中啟動。唯有使用完全吻合您 IT 組態的客製化沙盒環境，才能可靠地偵測客製化攻擊。

利用客製化沙盒來模擬您的真實 IT 環境，您就能：

- 發掘專門針對您的企業環境，如您的 Windows 授權、語言、應用程式以及桌上型電腦組合等等條件的
- 防止惡意程式使用一些根據通用 Windows 授權、少數標準應用程式版本以及英文等條件來判斷的沙盒
- 忽略一些不會對您環境造成影響的惡意程式，因為這些程式鎖定的是

Deep Discovery Analyzer 如何運作

前置處理單元 前置處理單元負責第一道偵測工作， 可解開壓縮的樣本檔案，判斷檔案的 真正類型而非仰賴附檔名來判斷，破 解初步的躲避技巧。

偵測引擎 利用多重偵測引擎，運用特徵與經驗 式掃瞄、趨勢科技 Smart Protection Network™信譽評等檢查、以及您 所定義的白名單和黑名單來分析並確 認檔案是否為惡意。

客製化沙盒模擬分析

Analyzer 可將未知與可疑的檔案傳送至最符合您環境的客製化沙盒中，安全地執行並分析潛在的惡意程式。然後將分析的結果回報給上傳者，包括風險指數與摘要。這些結果也可供管理員從 Analyzer 管理主控台執行進一 步的分析。

管理、分析與報表

Analyzer 主控台可以讓您執行深入的分析，並且產生摘要報表與個別樣本分析報表。在管理介面當中，您可以建立客製化沙盒系統影像、白名單與黑名單，並且根據檔案類型建立沙盒分析政策，例如自動對所有 PDF 檔案執行沙盒模擬分析。

Deep Discovery 平台

Deep Discovery Analyzer 是 Deep Discovery 系列環環相扣的產品之一，該系列提供網路、電子郵件、端點裝置與整合式防護，讓您在企業最關鍵的位置部署進階威脅防護。

客製化防禦

Deep Discovery 平台是趨勢科技 Custom Defense 客製化防禦的核心，將您的防護基礎架構建構成一套專為您企業量身訂做的完整防禦，對抗鎖定目標攻擊。

Deep Discovery 的客製化偵測、情報與控管能讓您：

- 偵測及分析攻擊者。
- 立即調整防護來反應攻擊。
- 快速因應以防止資料外洩。